PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

DoD OIG Information Technology Support (OIGITS) NIPRNet

2. DOD COMPONENT NAME:

Department of Defense Inspector General

3. PIA APPROVAL DATE:

02/11/25

Mission Support Team, Office of the Chief Information Officer (OCIO)

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)*

- ☐ From members of the general public
- ☐ From Federal employees
- ☒ from both members of the general public and Federal employees
- ☐ Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one.)*

- ☐ New DoD Information System
- ☐ New Electronic Collection
- ☒ Existing DoD Information System
- ☐ Existing Electronic Collection
- ☐ Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

The DoD OIG Information Technology Support (OIGITS) is an IT infrastructure that provides enterprise-wide authentication, messaging, backup and recovery, file and print services, application hosting, and enclave boundary security to obtain registration and provisioning data from the Defense Information Systems Agency (DISA). OIGITS is used to assign and manage security policies, computer servers, network devices, applications, user workstations, printers, and copiers.

OIGITS serves the DoD OIG headquarters and its field offices, to include those OCONUS. OIGITS has the capability to capture various types of PII, such as employee names, employment information, and military records, through the Electronic Data Interchange Personal Identifier (EDI-PI) or DoD ID number. OIGITS may also capture various PII data points from the general public when collection is made in connection with a complaint, an agency records request, official use request, audit, evaluation, or criminal or administrative investigation.

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

PII is collected for verification, identification, authentication, data matching, mission-related use, and administrative use.

e. Do individuals have the opportunity to object to the collection of their PII? ☐ Yes ☒ No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

PII collected in OIGITS is obtained via system-to-system interfaces. Additionally, DoD OIG personnel are added to the OIGITS enclave when IG Form 21, Network Access User Agreement, and DD Form 2875, System Authorization Access Request (SAAR), are submitted. Individuals granted access to OIGITS acknowledge and consent to routine intercepts and monitoring, inspection, and seizure of information within the enclave upon logging on to an OIG system.

f. Do individuals have the opportunity to consent to the specific uses of their PII? ☐ Yes ☒ No

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

DoD OIG personnel are added to the OIGITS enclave when both the IG Form 21 and DD Form 2875 are submitted. These forms do not contain a mechanism for individuals to limit the use of PII.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

☒ Privacy Act Statement ☐ Privacy Advisory ☐ Not Applicable

The OIGITS does not collect PII directly from any member of the public; however, when collection occurs, the following Privacy Act Statement applies:

AUTHORITY: 5 U.S.C. 407, Inspector General Act of 1978; 10 U.S.C. 2222, Defense Business Systems; Executive Order (E.O.) 10450, Security Requirements for Government Employment; E.O. 9397, Federal Agency Use of Social Security Numbers; Public Law 99-474, the Computer Fraud and Abuse Act of 1986; DoD Instruction (DoDI) 8500.01, Cybersecurity; DoDI 8520.03, Identity Authentication for Information Systems; and DoD OIG Instruction (IGDINST) 8170.04, Government Furnished Electronic Devices.
PURPOSE: To record names, signatures, and other identifiers for the purpose of validating the trustworthiness of individuals requesting access to DoD systems and information. NOTE: Records may be maintained in both electronic and/or paper form.
ROUTINE USE: In addition to the disclosures permitted by 5 U.S.C. 552a, Section (b), Conditions of Disclosure, information may be disclosed for any of the reasons listed in System of Records Notice DoD-0015, Enterprise Identity, Credential, and Access Management (ICAM) Records, published in the Federal Register at 87 F.R. 77085.
DISCLOSURE: Voluntary; however, failure to provide the requested information may impede, delay, or result in denial of access to DoD OIG information technology systems.

h. With whom will the PII be shared through data/system exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

☒ Within the DoD Component	Specify.	DoD OIG personnel with an established need-to-know that require access for mission requirements.
☒ Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.	Sharing is consistent with the Privacy Act, 5 U.S.C. 552a(b), Conditions of Disclosure, and the routine uses listed in SORN DoD-0015.
☒ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	Specify.	Sharing is consistent with the Privacy Act, 5 U.S.C. 552a(b), Conditions of Disclosure, and the routine uses listed in SORN DoD-0015.
☒ State and Local Agencies	Specify.	Sharing is consistent with the Privacy Act, 5 U.S.C. 552a(b), Conditions of Disclosure, and the routine uses listed in SORN DoD-0015.
☐ Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	
☒ Other *(e.g., commercial providers, colleges).*	Specify.	Sharing is consistent with the Privacy Act, 5 U.S.C. 552a(b), Conditions of Disclosure, and the routine uses listed in SORN DoD-0015.

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

☒ Individuals
☒ Existing DoD Information Systems
☐ Other Federal Information Systems
☒ Databases
☒ Commercial Systems

DoD OIG information systems and databases include Case Reporting and Information Management System (CRIMS), Defense Case Activity Tracking System Enterprise (DCATSe), Electronic Archive and Records Management System (EARMS), Digital Media Examination Network (DMEN), Evidence Tracking System (ETS), Contract Disclosure Program, Footprints, ServiceNow, DefenseReady, Exchange NIPR, Internet Defense Media Activity (DMA), Intranet Cold Fusion, Subpoena Program, Anti-Harassment Program, Kiteworks, OIGnet, SharePoint, and Teammate NIPR. DoD OIG personnel may also use commercial or publicly available data sources in the course of their official duties.

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

☒ E-mail
☐ In-Person Contact
☐ Fax
☒ Information Sharing - System to System
☐ Other *(If Other, enter the information in the box below)*
☒ Official Form (*Enter Form Number(s) in the box below)*
☒ Paper
☐ Telephone Interview
☐ Website/E-Form

PII is not collected directly from any member of the public. However, direct collection from DoD OIG personnel is made through IG Form 21 and DD Form 2875.

k. Does this DoD Information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information must be consistent.

☐ Yes ☒ No

If "Yes," enter SORN System Identifier

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

A SORN is not required as it is not an ordinary course of business to retrieve information in OIGITS using PII.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. GRS 4.2, 030; DAA-GRS-2019-0001-0002.

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

Temporary. Destroy 2 years after last form entry, reply, or submission; or when associated documents are declassified, decontrolled, or destroyed; or when an individual's authorization expires; whichever is appropriate. Longer retention is authorized if required for business use.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply).

(a) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) If direct or indirect authority does not exist, DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component must be identified.

5 U.S.C. 301, Regulations for the Government of the Department;
5 U.S.C. 407, Inspector General Act of 1978;
10 U.S.C. 2222, Defense Business Systems;
44 U.S.C. 3101, Records Management by Federal Agencies;
Executive Order 10450, Security Requirements for Government Employment;
Public Law 99-474, the Computer Fraud and Abuse Act of 1986;
DoD Instruction (DoDI) 5200.2, DoD Personnel Security Program;
DoDI 8500.1, Cybersecurity;
DoDI 8520.03, Identity Authentication for Information Systems;
DoD Directive 5015.2, DoD Records Management Program;
IG Instruction (IGINST) 5015.2, Records Management Program; and
IGINST 8170.04, Government Furnished Electronic Devices.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (OMB) Control Number?

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information. This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ Yes ☒ No ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

OMB Control Number not required; OIGITS does not collect records from 10 or more members of the public.